Functional Series 500: Management Services
ADS Chapter 544 - Technical Architecture Design, Development, and Management

544.1	Authority
544.2	Objective
544.3	Responsibility
544.4	Definitions
544.5	POLICY
544.5.1	TECHNICAL ARCHITECTURE DESIGN, DEVELOPMENT AND MANAGEMENT
E544.5.1	Technical Architecture Design, Development and Management
544.5.1a	TECHNICAL ARCHITECTURE WAIVERS
E544.5.1a	Technical Architecture Waivers
544.5.2	OFF-SITE CONTRACTOR CONNECTIVITY
E544.5.2	Off-Site Contractor Connectivity
544.5.2a	OFF-SITE AUTHENTICATION
E544.5.2a	Off-Site Authentication
544.5.2b	INTERNET SERVICE PROVIDER (ISP)
E544.5.2b	Internet Service Provider (ISP) N/A
544.5.2c	INTERNET E-MAIL
E544.5.2c	Internet E-Mail
544.5.2d	COMPUTER HARDWARE/SOFTWARE
E544.5.2d	Computer Hardware/Software N/A
544.5.2e	SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION
E544.5.2e	Sensitive But Unclassified (SBU) Information
544.5.3	MANAGEMENT OF AUTOMATION HARDWARE
E544.5.3	Management of Automation Hardware
544.5.3a	COMPUTER EQUIPMENT
E544.5.3a	Computer Equipment
544.5.4	PROCUREMENT/INVENTORY OF FEDERAL INFORMATION PROCESSING (FIP) RESOURCES
E544.5.4	Procurement/Inventory of Federal Information Processing (FIP) Resources - N/A
544.5.6	Supplementary Reference - N/A
544.7	Mandatory Reference

Functional Series 500: Management Services
ADS Chapter 544 - Technical Architecture Design, Development, and Management

544.1 Authority

1. Federal Acquisition Regulation, Section 39.101, Policy
2. Federal Information Processing Standards Publications (FIPS PUBS), Ch. 11-2 and 11-3

544.2 Objective

To provide the framework for the design, development, management, and use of the Agency's Technical Architecture which includes all information technology/information management activities involving more than one Agency user. This policy does not cover equipment or services acquired for Agency bilateral host country agreements and projects, i.e., computer technology that shall actually be turned over to the host country.

To provide the essential procedures for the design, development, management, and use of the Agency's Technical Architecture.

544.3 Responsibility

1. The Chief Information Officer (CIO): The CIO, in the Bureau for Management (M) is responsible for setting strategic goals for the Technical Architecture and resolving conflict among constituents and users of the architecture.

2. The Director, Office of Information Resources Management (M/IRM/OD): M/IRM/OD is responsible for the design, management, coordination, interpretation, and modification of the Agency's Technical Architecture for information technology (IT) activities. The Director is also responsible for maintaining the Agency's Common User Interface standard.

3. The Bureau for Management, Office of Information Resources Management (M/IRM): M/IRM is responsible for executing the policies and essential procedures for Off-site Contractor Connectivity and maintaining the underlying network systems to support off-site contractor connection requirements. M/IRM reserves the right to choose the most appropriate form of connectivity to ensure that the level of user functionality is met and provides the "best value" to USAID.

M/IRM is also responsible for maintaining Internet gateways and telecommunications entry points within the Ronald Reagan Building (RRB) to AIDNET and maintaining the firewall system and authentication server.

4. Contracting Officer Technical Representatives (COTRs): COTRs, with input from the responsible Technical Administrator (TA), are responsible for evaluating contractor access requests to ensure that they meet current Statement of Work (SOW) needs and serve USAID business needs in a cost-effective manner. COTRs are also responsible for notifying M/IRM of contractors who no longer need access to AIDNET within one week of departure.

COTRs are responsible for coordinating with the Office of the Inspector General, Office of Security (IG/SEC) to ensure that the appropriate security clauses are placed in the contract, including the requirement for approved background checks and security clearances of contractor personnel.

5. USAID Contractors: Contractors are responsible for maintaining their own computer equipment, network servers, routers, telecommunication connections (including Internet accounts) and software in their off-site locations.

Contractors are also responsible for protecting Agency information and data that is created, processed, stored and/or transmitted by their staff from unauthorized access. This includes protection from unauthorized distribution, modification, and destruction.

6. Agency Project Officers and Others: Officials who plan or manage activities that require automated exchange of information with other government agencies, vendors, contractors, or host country counterparts are responsible for planning activities for compatibility with the Agency's architecture which specifically addresses interoperability with other systems in ways compatible with relevant Federal Information Processing (FIP) standards.

7. Agency Managers: Managers are responsible for advising M/IRM of upcoming requirements to ensure that the architecture contains appropriate resources and is enhanced to fully support the Agency's business needs.

Officials who plan or manage Agency contracts that require vendors or contractors to supply information to the Agency must plan for the automation of this activity within the Agency's architecture. Contracts must specify appropriate media, format, and protocols for contractor-supplied information.

544.4 Definitions (**See GLOSSARY**)

Interoperability Lab
Open System
Technical Architecture For Information Technology (IT)

544.5 POLICY

The statements contained within the .5 section of this ADS chapter are the official Agency policies and corresponding essential procedures.

544.5.1 TECHNICAL ARCHITECTURE DESIGN, DEVELOPMENT AND MANAGEMENT

Agency computer systems shall use an open systems-based architecture.

Strategy to employ functional interoperability among the Agency's computer systems and accompanying ancillary components as capabilities become available. Agency computer systems shall be compatible with the existing Technical Architecture as defined by the Bureau for Management, Office of Information Resource Management (M/IRM), based on the OMB-mandated Information Technology Architecture (ITA) principles, guidelines, and tenets.

The ITA plan for the Agency shall reflect the Clinger-Cohen Act, i.e., Information Technology Management Reform Act (ITMRA) requirements for Federal Agency IT standards, policies and procedures. M/IRM's Information Policy and Administration Division (M/IRM/IPA) shall be the coordinating point for analysis, design, and testing of interpretation and modification of the Technical Architecture.

E544.5.1 Technical Architecture Design, Development and Management

Agency business managers, through M/IRM's Consulting and Information Services Division (M/IRM/CIS), as well as technical specialists responsible for operations, through the Bureau for Management, Office of Information Resource Management, Telecommunications and Computer Operations Division (M/IRM/TCO), must advise M/IRM/IPA of upcoming requirements to ensure that the Technical Architecture contains appropriate resources to fully support the Agency's business needs.

M/IRM shall design, develop and maintain the Agency's Technical Architecture which includes the following components:

a) Database Servers;
b) Personal Computer Hardware;
c) Personal Computer Operating Systems;
d) File Server Operating System;

e) Common User Interface (CUI);
f) Network Communications Software;
g) Telecommunications Links;
h) Electronic Mail (E-Mail);
i) Word Processing;
j) Text Standards; and
k) Network Engineering/Design and Management.

M/IRM shall validate the Agency's IT Technical Architecture on a regular basis to ensure compliance with technical standards, reference models, and enterprise network components.

M/IRM must be contacted for detailed specifications for each of the above architecture components.

544.5.1a TECHNICAL ARCHITECTURE WAIVERS

In circumstances where implementation of Technical Architecture standards are unduly restrictive, or not cost-effective, Agency managers must request a waiver of this standard. The Director of M/IRM has authority to grant waivers. The Director shall grant, deny, or seek further clarification of the waiver requested.

E544.5.1a Technical Architecture Waivers

To obtain a waiver to the Agency's Technical Architecture standards, Agency officials must contact and request a waiver from the Bureau for Management, Office of Information Resources Management, Office of the Director (M/IRM/OD).

544.5.2 OFF-SITE CONTRACTOR CONNECTIVITY

All contractors' off-site access to AIDNET must be reviewed and approved by M/IRM management. Contractors who are authorized access to AIDNET must have an approved background check or, if applicable, a security clearance and remote access authorization from the responsible Contracting Officer Technical Representative (COTR) before access is approved. This shall be the responsibility of the COTR for each contract.

All remote access to the network shall be controlled by firewalls in the Ronald Reagan Building (RRB). COTRs must provide M/IRM with detailed, system-level information on all remote users to properly configure these systems.

E544.5.2 Off-site Contractor Connectivity

Data collection forms shall be circulated to COTRs for basic connectivity information. Only those contractors with direct AIDNET application access requirements need to fill them out.

Only contractors who develop, maintain, or are required to access mission-critical systems for the Agency shall be considered for AIDNET connections from off-site locations. M/IRM shall evaluate such requests on a case-by-case basis and determine the type of connectivity that is warranted. Factors, such as the ability to use Internet, technical characteristics of systems developed, cost tradeoffs, security issues, and administrative costs shall be used to evaluate contractor requests.

COTRs must meet with contract TAs and contractor managers to determine if specific connectivity requests are warranted. For new hires, this step must be completed well in advance of the desired start date. All connectivity requirements, background checks, and authorization approvals must be completed before access is approved.

Upon review and approval by the COTR, contractor connectivity requests must be sent to M/IRM for technical review and the Bureau for Management, Office of Procurement (M/OP) if contract modifications are required.

If the request is approved, M/IRM shall request more detailed technical specifications, user authorization forms, and specific contractor location data from the COTR in order to connect users to AIDNET.

M/IRM shall support connectivity to the RRB for approved users via FNS connection (Bell Atlantic), SMDS/shared digital connection (Bell Atlantic), or dial-up/Remote Access Server (RAS). Other types of connections shall be considered on a case-by-case basis.

544.5.2a OFF-SITE AUTHENTICATION

All off-site/remote access to AIDNET shall require the use of authentication of an individual user via software being installed in the RRB. This software shall be distributed by the M/IRM Automated Information System Security Group once contractors have been approved by the responsible COTR.

E544.5.2a Off-site Authentication

M/IRM shall maintain the authentication software server to ensure that all valid users have proper accounts. The COTR shall be responsible for informing M/IRM when a Contractor no longer requires access to AIDNET.

544.5.2b INTERNET SERVICE PROVIDER (ISP)

USAID's public network Internet servers and data shall be accessible, via an Internet Service Provider (ISP) account, which is the responsibility of the Contractor. Personnel needing to update and maintain USAID-based Internet server data (including Intranet servers) shall request such access rights from M/IRM in the initial off-site connectivity request.

E544.5.2b Internet Service Provider (ISP) - N/A

544.5.2c INTERNET E-MAIL

M/IRM shall support Internet E-Mail for information, documents, and mail exchanged between off-site contractors and USAID staff in the RRB. Direct access to AIDNET systems shall not be provided to most off-site contractors.

E544.5.2c Internet E-Mail

M/IRM (and USAID in general) shall make every effort to protect the privacy of individual user information contained in electronic messages sent over the AIDNET; however, users must be aware that messages generated on AIDNET are subject to monitoring, whether authorized or unauthorized, and are subject to all applicable Federal government laws and regulations regarding electronic communications. These laws include provision of information to law enforcement officials, maintaining public records of communications within the normal course of business, and storage of electronic records for archival purposes. M/IRM shall assist the responsible USAID offices in meeting applicable Federal and Agency records management duties.

M/IRM shall make available the AIDNET-specific Internet specifications for E-Mail, attachments, etc., and provide assistance in connecting to the USAID Internet gateway to all off-site contractors. Contractors, however shall be expected to establish contractors' own Internet Service Provider (ISP) account.

544.5.2d COMPUTER HARDWARE/SOFTWARE

M/IRM shall not maintain or support computer hardware or software operating in off-site contractor location, nor provide Government-funded Equipment (GFE) to off-site contractors when relocated from USAID space. This shall be the responsibility of each contractor.

M/IRM shall provide Internet gateway configuration support, telecommunications connections, and maintain the firewall software in the

RRB used to connect off-site contractors.

E544.5.2d Computer Hardware/Software - N/A

544.5.2e SENSITIVE BUT UNCLASSIFIED INFORMATION (SBU)

Remote contractors shall adhere to the Agency's Sensitive But Unclassified (SBU) policy for safeguarding electronically formatted information.

E544.5.2e Sensitive But Unclassified Information (SBU)

Remote contractors shall adhere to Series 500, Interim Update **5**, dated February 3, 1997, entitled, Sensitive But Unclassified (SBU) Information Created, Processed, Stored, or Transmitted in Electronic Format **(See Mandatory Reference, Series 500, Interim Update 5, Sensitive But Unclassified (SBU) Information Created, Processed, Stored, or Transmitted in Electronic Format).** The SBU policies and essential procedures will be included in ADS Chapter 545, Automated Information Systems Security, in the September, quarterly update.

544.5.3 MANAGEMENT OF AUTOMATION HARDWARE

M/IRM/OD shall direct the ongoing strategic planning for the Agency's hardware and software architectures and development of the Agency's hardware architecture.

E544.5.3 Management of Automation Hardware

Agency project officers and others, who manage or plan activities dealing with automated exchange of information, must ensure that these activities are compatible with the Agency's architecture. Managers must inform M/IRM of new business requirements that significantly affect components of the Technical Architecture, such as multimedia training, video conferencing, collaborative workgroups, etc.

Officials, who plan or manage Agency contracts that require vendor or contractors to supply information to the Agency, must plan with M/IRM to ensure that such activities are compatible with the Agency's architecture.

544.5.3a COMPUTER EQUIPMENT/SOFTWARE

M/IRM shall have overall authority for determining, establishing, and enforcing acceptable levels of operational support for all computer equipment in the Agency.

M/IRM shall assign responsibility for day-to-day operation of computer equipment, depending on the computing environment, support levels required, relative degree of control required, and overall interest of the Agency.

All USAID/W computer equipment located in USAID/W shall be maintained by M/IRM. Mission Directors shall oversee the operation of computer hardware at overseas locations.

E544.5.3a Computer Equipment/Software

USAID -owned and-leased hardware shall be used only for conducting official government business.

Only M/IRM approved software shall be installed on Agency computers. No personal software shall be installed on Agency computers.

Resource use must be monitored by the computer operations manager to track usage and malfunctions of devices. Resource accounting must be used to assist computer operations managers in analyzing the equipment's overall performance and estimating client usage of computers.
Problems encountered with equipment, which end-users cannot solve, must first be reported to M/IRM's Information Technology (IT) Specialists. If M/IRM's assistance is required, problems must be reported to M/IRM/TCO.

Officials responsible for the operation of equipment must ensure that all software and data are backed up on a regular basis, preferably no less than once a week and always before major adjustments are made to either the equipment or software. In cases where M/IRM intends to change or enhance hardware or software, M/IRM must run the necessary backup procedures or request the organizational unit's IT Specialist to do so. Backup media must be stored at a site other than the location of the computer.

Guidance contained in M/IRM's ADS Chapter 545, Automated Information System Security, must be followed regarding accessing Agency computers, environmental controls, physical security measures, fire detection/suppression devises, power support devices, access to facilities, and computer viruses **(See ADS 545)**.

Controls for access and use of Agency hardware shall be maintained by those responsible for operating the equipment.

544.5.4 PROCUREMENT/INVENTORY OF FEDERAL INFORMATION

PROCESSING (FIP) RESOURCES

In accordance with ADS Chapters 546, Acquisition of Operating Expense (OE)-Funded FIP Resources and 547, Property Management of FIP Resources, the inventory of FIP resources shall be reviewed, prior to procurement of FIP resource, to avoid acquisition of equipment already available for use **(See ADS 546 and 547)**.

E544.5.4 Procurement/Inventory of Federal Information Processing (FIP) Resources - N/A

544.6 Supplementary Reference - N/A

544.7 Mandatory Reference

ADS 545

ADS 546

ADS 547

Public Law (P.L.) 104-106 (Clinger-Cohen Act)

Series 500, Interim Update 5, Sensitive But Unclassified (SBU) Information Created, Processed, Stored, or Transmitted in Electronic Format

Glossary Terms for 544

Interoperability Lab
A vehicle for testing software and hardware policy reliability and compatibility before full-scale implementation. (Chapter 544)

Open System
A system capable of communicating with other open systems by virtue of implementing common international standard protocols. An open system is not always accessible by all other open systems. This isolation is either provided by physical separation or by technical capabilities based upon computer and communications security. (Chapter 544)

Technical Architecture for Information Technology (IT)

The conceptual model of USAID's information technology equipment/hardware, computer software, telecommunications and procedures which go together to build a fully functional information system. The Technical Architecture identifies the need for a resource, such as a computer, communications device, or a problem isolation procedure and also identifies feasible products that meet the need. (Chapter 544)